(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 février 2007 (01.02.2007)

PCT

(10) Numéro de publication internationale
WO 2007/012583 A1

(51) Classification internationale des brevets :
H04L 9/32 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2006/064383

(22) Date de dépôt international : 18 juillet 2006 (18.07.2006)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0507990 26 juillet 2005 (26.07.2005) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **ARDITTI, David** [FR/FR]; 46 ter, rue Paul Vaillant-Couturier, F-92140 Clamart (FR). **FRISCH, Laurent** [FR/FR]; 27 avenue d'Italie, F-75013 Paris (FR). **SIBERT, Hervé** [FR/FR]; 17, rue Robert le Magnifique, F-14000 Caen (FR).

(74) Mandataire : **BIORET, Ludovic**; 90333, 16b rue de Jouanet, F-35703 Rennes Cedex 7 (FR).

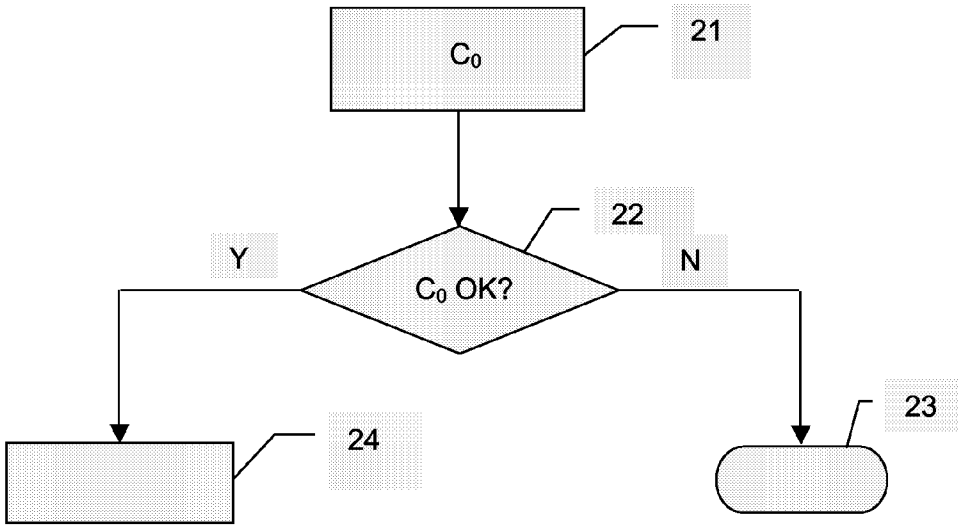
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Suite sur la page suivante]

(54) **Title:** METHOD FOR CONTROLLING SECURE TRANSACTIONS USING A SINGLE PHYSICAL DEVICE, CORRESPONDING PHYSICAL DEVICE, SYSTEM AND COMPUTER PROGRAMME

(54) **Titre :** PROCEDE DE CONTROLE DE TRANSACTIONS SECURISEES METTANT EN OEUVRE UN DISPOSITIF PHYSIQUE UNIQUE, DISPOSITIF PHYSIQUE, SYSTEME, ET PROGRAMME D'ORDINATEUR CORRESPONDANTS



(57) **Abstract:** The invention concerns a method for controlling secure transactions using a physical device (13) held by a user and bearing at least one pair of asymmetric keys, comprising a device public key (P_0) and a corresponding device private key (S_0). The invention is characterized in that said method includes the following steps: prior to implementing the physical device, a step of certifying said device public key (P_0) with a first certification key (S_T) of a particular certifying authority (10), delivering a device certificate (C_0) after verifying that said device private key (S_0) is housed in a tamper-proof zone of said physical device (13); a step of verifying said device certificate (C_0) by means of a second certification key (P_T) corresponding to the first certification key (S_T); in case of positive verification, a step of registering said user with a provider delivering a provider certificate (C_i) corresponding to the signature by said provider of said device public key (P_0) and an identifier (Id_i) of said user.

[Suite sur la page suivante]

WO 2007/012583 A1

FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de contrôle de transactions sécurisées mettant en œuvre un dispositif physique (13) détenu par un utilisateur et portant au moins une paire de clés asymétriques, comprenant une clé de dispositif publique (P_0) et une clé de dispositif privée (S_0) correspondante. Selon l'invention, un tel procédé comprend les étapes suivantes : préalablement à la mise en service dudit dispositif physique, une étape de certification de ladite clé de dispositif publique (P_0) par une première clé de certification (S_T) d'une autorité de certification particulière (10), délivrant un certificat de dispositif (C_0), après vérification que ladite clé de dispositif privée S_0 est logée dans une zone inviolable dudit dispositif physique (13) ; une étape de vérification dudit certificat de dispositif (C_0) au moyen d'une deuxième clé de certification (P_T) correspondant à ladite première clé de certification (S_T) ; - en cas de vérification positive, une étape d'enregistrement dudit utilisateur auprès d'un prestataire délivrant un certificat de prestataire (C_i) correspondant à la signature par ledit prestataire de ladite clé de dispositif publique (P_0) et d'un identifiant (Id_i) dudit utilisateur.

Procédé de contrôle de transactions sécurisées mettant en œuvre un dispositif physique unique, dispositif physique, système, et programme d'ordinateur correspondants.

1. Domaine de l'invention

Le domaine de l'invention est celui de la sécurisation des transactions électroniques, mettant notamment en œuvre des opérations d'authentification, de signature électronique et de paiement, effectuées par le biais de réseaux de communication tels que le réseau Internet par exemple.

Plus précisément, l'invention concerne une technique de contrôle de transactions sécurisées faisant intervenir un dispositif physique détenu par un utilisateur.

2. Solutions de l'art antérieur

Le fort développement des réseaux de communication, comme le réseau mondial Internet par exemple, et l'accroissement constant du nombre de transactions effectuées chaque jour sur ces réseaux, a fait naître un besoin sans cesse croissant de sécurisation des transactions. En effet, il est apparu nécessaire de reproduire sur ces réseaux informatiques ou de radiocommunication l'environnement de confiance entourant les échanges physiques par courrier classique ou par contact direct.

Selon l'art antérieur, un certificat permet notamment de vérifier la validité d'une clé cryptographique publique utilisée sur un réseau informatique, et est un message comprenant, au minimum, une clé publique, un identifiant de son détenteur, une période de validité, une identification d'une autorité de certification, ainsi qu'une signature cryptographique de ces différentes données, réalisée au moyen de la clé secrète de cette autorité de certification émettrice du certificat.

La lecture du certificat permet d'authentifier avec certitude l'émetteur d'un message reçu dans le cas de la signature et l'identifiant de celui qui s'authentifie dans le cas de l'authentification.

Pour plus d'information sur les certificats, on pourra se référer notamment

au standard X.509, et plus particulièrement X.509v3 défini dans la RFC3280 (Request For Comment n°3280) publiée par l'IETF (Internet Engineering Task Force).

Un inconvénient de cette technique de l'art antérieur est qu'elle ne permet pas à un prestataire de s'assurer simplement, et à distance, que le certificat de prestataire C qu'il délivre certifie bien une clé publique P_0 correspondant à une clé privée S_0 stockée dans un dispositif physique donné.

En effet, le comportement d'un dispositif physique peut être totalement simulé par un logiciel si bien qu'à distance, il est impossible pour le prestataire de savoir s'il correspond à un dispositif physique ou bien à une émulation logicielle d'un tel dispositif.

Or il existe plusieurs circonstances dans lesquelles il est important pour un prestataire d'avoir la preuve qu'il dialogue avec un véritable dispositif physique.

En effet, si la clé privée S_0 du dispositif physique reste stockée, conformément aux "bonnes pratiques", dans une zone secrète et inaccessible, le dispositif physique ne peut être cloné, et constitue donc un objet unique, qui est seul capable de produire les authentifiants et les signatures correspondant à la clé publique P_0, donc au certificat C_i, et donc également à l'identifiant Id_i par lequel le client est connu du $i^{ième}$ prestataire. Le possesseur du dispositif physique est alors le seul à pouvoir s'authentifier ou signer avec l'identifiant Id_i vis-à-vis du $i^{ième}$ prestataire, ce qui constitue une propriété de non-répudiation forte, gage de sécurité pour le prestataire.

Une autre circonstance dans laquelle il est important pour le prestataire de pouvoir s'assurer qu'il a affaire à un dispositif physique donné est le cas où ce dispositif physique est le support d'un abonnement payant à un service fourni par le prestataire (par exemple, l'accès sur Internet aux articles de journaux publiés dans un quotidien). L'accès au service payant est conditionné, pour l'utilisateur, par l'ouverture d'une session auprès du prestataire, au cours de laquelle il s'authentifie au moyen de son dispositif physique.

Il est donc particulièrement important pour le prestataire de s'assurer que le

client qui souhaite accéder au service est bien en possession du dispositif physique, afin d'éviter que plusieurs personnes puissent accéder (simultanément ou non) au service, en payant un seul abonnement, ce qui serait le cas si le support de l'abonnement pouvait être cloné (par exemple si le support de l'abonnement était un ensemble "identifiant/mot de passe" ou une clé privée (même chiffrée) stockée sur un disque dur).

La demande de brevet français FR 96 08692 intitulée "Procédé de contrôle de transactions sécurisées indépendantes utilisant un dispositif physique unique", au nom du même demandeur que la présente demande de brevet, décrit plus particulièrement l'utilisation d'un tel dispositif physique pour réaliser une authentification auprès d'un ou plusieurs prestataires, avec lesquels l'utilisateur du dispositif souhaite effectuer une transaction.

Selon ce procédé, on met à la disposition des utilisateurs des dispositifs physiques tels que des cartes à puce ou des "dongles" USB ("Universal Serial Bus" pour "bus série universel"), qui sont classiquement associés à une paire de clés asymétriques (P_0, S_0) comprenant une clé privée S_0 et une clé publique P_0. La clé privée S_0 est un élément électronique qui doit rester secret, et qui est donc stocké dans un espace protégé du dispositif physique, à l'abri de toute tentative d'intrusion. La clé publique P_0 quant à elle peut être stockée en lecture libre dans le dispositif physique, ou être livrée à l'utilisateur sur un support externe, tel qu'une disquette, un CD-Rom, un document papier, ou un espace réservé d'un serveur de données. Cette paire de clés (S_0, P_0) est créée en usine, préalablement à la commercialisation et à la mise en service du dispositif.

Un tel dispositif physique comprend également classiquement des moyens de calcul permettant de mettre en œuvre un algorithme cryptographique asymétrique d'authentification et/ou de signature. Parmi ces algorithmes, on peut citer les algorithmes de type RSA (Rivest-Shamir-Adleman), DSA, GQ (Guillou-Quisquater) ou GPS par exemple.

L'utilisation de cet algorithme cryptographique asymétrique peut être assujetti à la présentation préalable d'un code porteur (ou code PIN pour "Personal

Identification Number") initialisé lors d'une phase de (pré-)personnalisation du dispositif physique, et géré selon des techniques classiques qui ne font pas l'objet de la présente demande de brevet.

Le dispositif physique peut être ensuite vendu sous cette forme à un utilisateur, par un moyen de distribution indépendant de tout prestataire.

Pour pouvoir réaliser une transaction sécurisée (authentification, signature) avec un prestataire, l'utilisateur du dispositif physique, encore appelé client, doit se faire délivrer par le prestataire un certificat de prestataire C_1 liant la clé publique P_0 du dispositif et un identifiant Id_1 pertinent pour le prestataire (Remarque: dans les systèmes où l'anonymat de l'utilisateur vis-à-vis du prestataire doit être préservé, l'identifiant Id_1 est différent de l'identité civile de l'utilisateur).

Cette opération, couramment appelée "enregistrement", peut être réalisée auprès de n prestataires distincts, de sorte que le client se voit attribuer n certificats de prestataire $\{C_1, C_2,\ldots,C_n\}$ liant n identifiants $\{Id_1, Id_2,\ldots, Id_n\}$ (chacun d'entre eux étant pertinent pour un prestataire donné) avec la même clé publique P_0.

Lorsqu'il veut ensuite réaliser une transaction sécurisée avec le $i^{ième}$ prestataire, le client utilise son dispositif physique pour signer un aléa envoyé par le prestataire (on parle alors d'authentification) ou un message (on parle alors de signature électronique) grâce à sa clé secrète S_0 et en y associant le certificat correspondant C_i fourni par le prestataire, selon des protocoles standardisés.

3. Inconvénients de l'art antérieur

Selon la technique antérieure, la seule solution permettant à un prestataire de s'assurer que la transaction en cours se fait bien au moyen d'un dispositif physique donné repose sur la manipulation physique du dispositif par le prestataire. En effet, il peut alors lire lui-même la clé publique P_0 dans le dispositif, dans le cas où elle y est stockée. Dans le cas contraire, il peut faire signer un aléa au dispositif, au moyen de la clé secrète S_0, et vérifier ensuite le résultat de cette signature au moyen de la clé publique P_0 fournie par le client sur

un support externe.

Cependant, un inconvénient de cette solution antérieure est qu'elle impose que le prestataire puisse opérer physiquement sur le dispositif, et exclut donc toute action à distance, ce qui s'avère très problématique dans le cadre de transactions effectuées sur les réseaux de communication modernes tels qu'Internet.

4. Objectifs de l'invention

L'invention a notamment pour objectif de pallier ces inconvénients de l'art antérieur.

Plus précisément, un objectif de l'invention est de fournir une technique de contrôle de transactions sécurisées mettant en œuvre un dispositif physique associé à une paire de clés asymétriques (P_0, S_0), permettant de s'assurer simplement et éventuellement à distance qu'une transaction est bien effectuée au moyen d'un dispositif physique donné.

En d'autres termes, l'invention a pour objectif de proposer une telle technique qui permette à un prestataire de s'assurer que la clé publique P_0 qu'il doit certifier correspond bien à une clé secrète S_0 stockée dans un dispositif physique donné.

Un autre objectif de l'invention est de proposer une telle technique qui soit simple à mettre en œuvre et n'introduise pas ou peu de complexité supplémentaire dans les dispositifs physiques utilisés.

L'invention a encore pour objectif de fournir une telle technique qui soit fiable et permette d'obtenir une propriété de non répudiation forte, de façon à créer, pour le prestataire, un environnement de confiance.

5. Exposé de l'invention

Ces objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints à l'aide d'un procédé de contrôle de transactions sécurisées mettant en œuvre un dispositif physique détenu par un utilisateur et portant au moins une paire de clés asymétriques, comprenant une clé de dispositif publique (P_0) et une clé de dispositif privée (S_0) correspondante.

Selon l'invention, un tel procédé comprend les étapes suivantes :

- préalablement à la mise en service dudit dispositif physique, une étape de certification de ladite clé de dispositif publique (P_0) par signature au moyen d'une première clé de certification (S_T) d'une autorité de certification particulière (ACP), délivrant un certificat de dispositif (C_0), après vérification que ladite clé de dispositif privée S_0 est logée dans une zone inviolable dudit dispositif physique (13) ;
- une étape de vérification dudit certificat de dispositif (C_0) au moyen d'une deuxième clé de certification (P_T) correspondant à ladite première clé de certification (S_T);
- en cas de vérification positive, une étape d'enregistrement dudit utilisateur auprès d'un prestataire délivrant un certificat de prestataire (C_i) correspondant à la signature par ledit prestataire de ladite clé de dispositif publique (P_0) et d'un identifiant (Id_i) de cet utilisateur.

Ainsi, l'invention repose sur une approche tout à fait nouvelle et inventive de la sécurisation de transactions électroniques. En effet, la technique de l'invention fait intervenir, pour introduire un degré supplémentaire de sécurisation, une autorité de certification particulière (ACP), à laquelle les différents prestataires accordent toute leur confiance. Cette autorité de certification particulière délivre, préalablement à la mise en service du dispositif physique ("dongle" USB, carte à puce, ...), un certificat relatif à ce dispositif physique (et non comme dans l'art antérieur un certificat relatif à un identifiant de son détenteur), dont la vérification de la validité est une garantie, pour le prestataire, qu'il se trouve, même à distance, en présence d'un véritable dispositif physique, et non d'un équipement (ordinateur, PDA, etc.) qui en reproduirait frauduleusement le comportement.

Cette sécurisation repose sur un engagement fort, de la part de l'autorité de certification particulière, de ne produire de tels certificats de dispositif C_0 à partir d'une première clé de certification S_T, que pour des clés publiques P_0 correspondant à des clés privées S_0 stockées dans un dispositif physique donné.

La vérification du certificat de dispositif peut être effectuée directement

par le prestataire, à partir d'une deuxième clé de certification de l'autorité de certification particulière que celle-ci lui aura communiquée, ou par un tiers de confiance. Ainsi, le procédé de contrôle de transactions selon l'invention utilise l'engagement de l'ACP pour assurer à un prestataire qu'un client qui souhaite engager une transaction sécurisée possède bien un dispositif physique, lequel a été certifié par l'ACP. On se distingue ainsi fortement de l'art antérieur, qui n'assure pas à distance que l'utilisateur possède un dispositif physique. En effet, les techniques de contrôles selon l'art antérieur assurent seulement l'identification d'un utilisateur, si besoin à l'aide d'un enchaînement d'authentifications et de certifications basé sur l'utilisation d'une succession d'autorités de certification, mais ayant toujours pour unique conséquence la certification de l'identité d'un utilisateur. Le procédé selon l'invention comprend, outre la certification de l'identité de l'utilisateur, la certification préalable du dispositif physique subséquemment détenu par cet utilisateur. Cela permet d'assurer à un prestataire, éventuellement à distance, que l'utilisateur qui s'authentifie auprès de lui possède un dispositif physique. Seule cette assurance permet la poursuite de l'établissement du processus de contrôle de transaction.

Lorsqu'il est assuré de la validité du certificat de dispositif C_0, le prestataire peut alors procéder classiquement à l'enregistrement de l'utilisateur, auquel il délivre un certificat de prestataire C_i.

De manière préférentielle, ladite autorité de certification particulière est le fabricant dudit dispositif physique, qui peut alors délivrer le certificat de dispositif C_0, directement en sortie des chaînes de fabrication. Il peut bien sûr également s'agir d'une autorité de certification tierce, travaillant pour un ou plusieurs fabricants distincts.

Avantageusement, ledit certificat de dispositif C_0 est stocké dans une zone de mémoire en lecture libre dudit dispositif physique. Il peut ainsi aisément être vérifié par le prestataire.

Selon une caractéristique avantageuse de l'invention, ledit certificat de dispositif C_0 signe également au moins une information représentative dudit

dispositif physique, qui appartient au groupe comprenant les informations suivantes :

- type de dispositif physique ;
- identification du fabricant dudit dispositif physique ;
- type d'algorithme cryptographique utilisé par ledit dispositif physique ;
- numéro de série dudit dispositif physique.

Lors de la vérification du certificat de dispositif C_0, le prestataire dispose ainsi d'informations complémentaires sur le dispositif physique auquel il a affaire, qui peuvent lui permettre par exemple de vérifier que le type du dispositif convient à la nature de la transaction envisagée, ou d'assurer la traçabilité du dispositif, à partir de son numéro de série.

Selon une variante de réalisation avantageuse de l'invention, ladite étape de vérification est effectuée par ledit prestataire. Ainsi, le prestataire sait directement s'il peut ou non procéder à l'enregistrement de l'utilisateur, sans avoir à faire appel à une autorité de vérification tierce (ce qui pourrait également être envisagé dans le cadre de la présente invention).

Dans un premier mode de réalisation avantageux de l'invention, ladite première clé de certification S_T est une clé privée et ladite deuxième clé de certification P_T est une clé publique. On utilise ainsi une paire de clés asymétriques, dont la clé privée S_T est gardée secrète par l'autorité de certification particulière, au contraire de la clé publique qui peut être communiquée aux prestataires ou publiée.

Dans un deuxième mode de réalisation avantageux de l'invention, ladite autorité de certification particulière utilise une clé symétrique K, de sorte que ladite première clé de certification S_T et ladite deuxième clé de certification P_T sont identiques.

Dans ce cas, ladite étape de certification est mise en œuvre à partir de ladite clé symétrique par ladite autorité de certification particulière sur requête d'un fabricant dudit dispositif, et ladite étape de vérification est mise en œuvre par ladite autorité de certification particulière sur requête dudit prestataire.

A nouveau, cette autorité de certification particulière peut bien sûr être le fabricant lui-même.

L'invention concerne aussi un dispositif physique détenu par un utilisateur et destiné à être utilisé lors de transactions sécurisées, ledit dispositif physique portant au moins une paire de clés asymétriques, comprenant une clé de dispositif publique P_0 et une clé de dispositif privée S_0 correspondante.

Selon l'invention, un tel dispositif porte également un certificat de dispositif C_0, délivré après vérification que ladite clé de dispositif privée S_0 est logée dans une zone inviolable dudit dispositif physique (13), correspondant à la signature de ladite clé de dispositif publique P_0 par une première clé de certification S_T d'une autorité de certification particulière,
et ledit certificat de dispositif C_0 est stocké dans ledit dispositif physique préalablement à sa mise en service.

L'invention concerne aussi un produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour la mise en œuvre d'au moins une étape du procédé de contrôle de transactions sécurisées décrit précédemment.

L'invention concerne encore un système de contrôle de transactions sécurisées sur un réseau de communication, mettant en œuvre un dispositif physique détenu par un utilisateur et portant au moins une paire de clés asymétriques, comprenant une clé de dispositif publique P_0 et une clé de dispositif privée S_0 correspondante. Un tel système comprend au moins :

- un serveur de certification particulière relié audit réseau, délivrant audit dispositif physique, après vérification que ladite clé de dispositif privée S_0 est logée dans une zone inviolable dudit dispositif physique (13) et préalablement à sa mise en service, un certificat de dispositif C_0 correspondant à la signature de ladite clé de dispositif publique P_0 par une première clé de certification S_T dudit serveur de certification particulière ;

- un serveur de vérification dudit certificat de dispositif C_0 au moyen d'une deuxième clé de certification P_T correspondant à ladite première clé de certification S_T, ledit serveur de vérification étant relié audit réseau ;
- un serveur d'enregistrement dudit utilisateur auprès d'un prestataire, délivrant audit utilisateur, en cas de vérification positive par ledit serveur de vérification, un certificat de prestataire C_i correspondant à la signature par ledit prestataire de ladite clé de dispositif publique P_0 et d'un identifiant Id_i dudit utilisateur, ledit serveur d'enregistrement étant relié audit réseau.

6. Liste des figures

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 illustre le principe de la certification, par une autorité de certification particulière, de la clé publique d'un dispositif physique, préalablement à sa mise en service ;
- la figure 2 présente un synoptique des différentes étapes mises en œuvre dans le procédé de contrôle de transactions sécurisées de l'invention ;
- la figure 3 décrit les différents échanges entre un utilisateur et différents serveurs de l'invention, via un réseau de communication, dans le cadre du procédé de la figure 2.

7. Description d'un mode de réalisation de l'invention

Le principe général de l'invention repose sur la certification de la clé publique P_0 d'un dispositif physique, préalablement à sa mise en service, par une autorité de certification particulière, permettant de garantir à un prestataire, lors d'une transaction sécurisée (éventuellement à distance), qu'il traite bien avec un véritable dispositif physique, dans lequel est stockée la clé privée S_0 associée à la clé publique P_0.

On présente, en relation avec la figure 1, un mode de réalisation de la certification de la clé publique P_0 d'un dispositif physique 13 donné,

préalablement à sa mise en service.

Une autorité de certification particulière, ou ACP, 10 possède une paire de clés asymétriques (P_T, S_T) comprenant une clé publique P_T et une clé privée S_T conservée dans une zone secrète et inaccessible 101. Une telle ACP 10 est par exemple le fabricant du dispositif physique : la zone secrète 101 dans laquelle est mémorisée la clé privée S_T est alors un dispositif physique particulier (une carte à puce par exemple) détenu par le fabricant, ou une zone mémoire protégée à accès restreint de l'un de ses équipements informatiques.

La clé publique P_T quant à elle est publiée par l'ACP 10, ou fournie à la demande à des prestataires potentiels susceptibles d'en avoir besoin (i.e. aux prestataires susceptibles de réaliser des transactions avec le détenteur du dispositif physique 13).

Lors de la fabrication du dispositif physique 13, on y enregistre une paire de clés asymétriques (P_0, S_0) comprenant une clé publique P_0, mémorisée dans une zone 131 accessible en lecture du dispositif 13, et une clé privée S_0 mémorisée dans une zone protégée 132 de ce dispositif 13. Cette zone protégée, ou inviolable, 132 est conçue de façon à empêcher la lecture de la clé privée S_0 et à résister à toute tentative d'intrusion logicielle ou matérielle. En variante, la clé publique P_0 peut également être communiquée au détenteur du dispositif physique 13 sur un support externe, indépendant du dispositif lui-même.

Si l'ACP 10 est le fabricant du dispositif physique 13, les opérations illustrées sur la figure 1 sont réalisées avant la commercialisation du dispositif physique, en usine, lors d'une phase de (pré-)personnalisation du dispositif. S'il s'agit d'une autorité de certification indépendante du fabricant, ces opérations peuvent être réalisées en sortie des chaînes de fabrication, avant la distribution des dispositifs physiques aux utilisateurs finaux.

Plus précisément, le dispositif physique 13 communique 11 à l'ACP 10 sa clé publique P_0. L'ACP 10 signe alors avec sa clé privée S_T la clé publique P_0 du dispositif 13. Cette signature 12 constitue un certificat d'identité $C_0=A(S_T,P_0)$ (où A désigne un algorithme cryptographique de signature, de type RSA par exemple)

qui, comme la clé publique P_0 pourra être inscrite dans le dispositif physique 13, dans une zone en lecture libre 131, ou fournie à l'utilisateur du dispositif 13 sur un support externe (disquette, CD-Rom, document papier, ...).

L'ACP 10 (fabricant ou tiers de confiance) s'engage bien sûr à ne produire de tels certificats de dispositif C_0 (i.e. de telles signatures avec sa clé privée S_T) que pour des clés publiques P_0 correspondant à des clés privées stockées dans un dispositif physique d'un type donné.

Les opérations de certification de la figure 1 peuvent également, dans une variante de réalisation de l'invention, être mutualisées pour plusieurs fabricants de dispositifs physiques de types différents. Dans ce cas, l'ACP 10 est un tiers de confiance indépendant de l'ensemble des fabricants, qui détient la clé privée S_T et qui, pour produire le certificat de dispositif C_0 d'un dispositif physique 13 donné, signe, avec sa clé privée S_T, le couple (P_0, <type du dispositif>). Une telle information <type du dispositif> permet de renseigner par exemple sur la nature du dispositif 13, à savoir un "dongle" USB, une carte à puce, etc. Il peut également s'agir de la référence produit utilisée par le fabricant pour désigner l'un des dispositifs qu'il construit.

De même, en variante, d'autres informations pertinentes pour l'utilisation du dispositif physique 13 peuvent être signées dans le certificat du dispositif C_0, telles que le nom du fabricant (<nom du fabricant>), le type d'algorithme cryptographique utilisé (<type d'algorithme>), le numéro de série du dispositif, etc.

Ainsi, lors d'une phase ultérieure de vérification du certificat de dispositif C_0 par un prestataire (décrite ci-dessous plus en détail en relation avec les figures 2 et 3), ce dernier sera assuré que la clé publique P_0 correspond à une clé secrète S_0 stockée dans un dispositif 13 de type <type du dispositif>, fabriqué par <nom du fabricant>, et utilisant l'algorithme cryptographique <type d'algorithme>. Cette assurance résulte de la confiance qu'a le prestataire en l'autorité de certification particulière 10.

On peut également imaginer, en variante des opérations illustrées par la

figure 1, que $P_T=S_T=K$ soit une clé symétrique.

Dans ce cas, la clé K peut être partagée entre le fabricant du dispositif physique 13 et un (ou quelques rares) tiers de confiance, dont le fabricant sait qu'ils garderont cette clé K secrète ; dans ce cas, seuls ces tiers ou le fabricant lui-même pourront vérifier le certificat.

On peut aussi envisager que la clé K ne soit utilisée que par une ACP 10 indépendante du fabricant, qui signe le certificat de dispositif C_0 à clé symétrique, uniquement sur demande du fabricant de dispositifs physiques 13. De même, cette ACP 10 sera seule à pouvoir vérifier les certificats de dispositif C_0, sur requête des prestataires souhaitant réaliser une transaction avec les dispositifs physiques 13 associés. A nouveau, cette ACP 10 peut bien sûr être le fabricant lui-même.

Le dispositif physique 13 dans lequel le certificat C_0 a été enregistré par l'ACP 10 est vendu par un moyen de distribution indépendant de tout prestataire, par exemple dans une grande surface ou chez un revendeur agréé.

On présente désormais, en relation avec les figures 2 et 3, la façon dont le certificat de dispositif C_0 est utilisé dans le cadre d'une transaction sécurisée entre le possesseur 30 du dispositif physique 13 et un prestataire 33. Un tel prestataire 33 peut être par exemple un prestataire de services (accès à un service météo, ou à un service de géolocalisation par exemple) ou un vendeur de biens (commerçant sur Internet par exemple).

Le dispositif physique 13 a été acquis par un utilisateur 30, qui souhaite par exemple l'utiliser pour accéder aux services proposés par un prestataire 33, via un réseau de communication 32, par exemple le réseau mondial Internet. Un tel dispositif physique 13 sert par exemple de support à un abonnement payant souscrit par l'utilisateur 30 auprès du prestataire 33 (par exemple un abonnement à un horoscope quotidien publié sur Internet).

L'utilisateur 30, lorsqu'il souhaite accéder aux services du prestataire 33, émet, via son terminal de communication 31 (e.g. un ordinateur), une requête, véhiculée par le réseau de communication 32, à destination du prestataire 33. Cette requête s'accompagne de la clé publique P_0 et du certificat de dispositif C_0

qui a été préenregistré 21 par l'ACP 10 dans le dispositif physique 13 (qui, par souci de simplification, n'a pas été représenté sur la figure 3).

Avant d'accéder à la requête de l'utilisateur 30, le prestataire veut vérifier que la clé publique P_0 qui lui a été transmise correspond bien à une clé secrète S_0 stockée dans un dispositif physique donné. Pour ce faire, il procède à une vérification 22 du certificat de dispositif C_0 transmis avec la requête, au moyen de la clé publique P_T de l'autorité de certification particulière 10.

En cas de vérification négative, c'est-à-dire si le certificat de dispositif C_0 ne correspond pas à la signature de la clé publique P_0 du dispositif physique par la clé privée S_T de l'ACP 10, le prestataire 33 peut mettre fin 23 à la transaction, et refuser l'accès de l'utilisateur 30 au bien ou au service demandé.

En cas de vérification positive en revanche, le prestataire 33 acquiert la certitude que la clé publique P_0 correspond bien à une clé privée S_0 stockée sur un dispositif physique 13 donné, et il peut donc accéder à la demande de l'utilisateur 30, en procédant à l'enregistrement 24 de ce dernier sous un identifiant pertinent (Id_i). Pour ce faire, le prestataire 33 délivre à l'utilisateur 30 un certificat de prestataire C_i correspondant à la signature de la clé publique P_0 et dudit identifiant (Id_i) par le prestataire 33. Ce certificat de prestataire C_i est transmis au terminal de communication 31 de l'utilisateur par le biais du réseau de communication 32 auquel est connecté le serveur d'enregistrement du prestataire 33.

La vérification 22 du certificat de dispositif C_0 peut être effectuée par le prestataire 33 lui-même ou par un serveur de vérification dédié 34, également connecté au réseau 32. Dans ce cas, le prestataire 33 transmet le certificat de dispositif C_0 au serveur de vérification 34 par le biais du réseau 32. Le serveur de certification 35 de l'ACP 10, qui a créé le certificat de dispositif C_0 du dispositif physique 13, communique ou a communiqué sa clé publique P_T au serveur de vérification 34. Le serveur de vérification 34 n'a plus qu'à utiliser la clé publique P_T du serveur de certification 35 pour vérifier l'authenticité du certificat C_0, puis transmettre le résultat de cette vérification au prestataire 33, afin que ce dernier sache s'il peut procéder à l'enregistrement 24 de l'utilisateur 30 ou s'il doit mettre

fin 23 à l'échange en cours.

Lorsque l'enregistrement 24 de l'utilisateur 30 auprès du prestataire a été effectué, l'utilisateur peut alors commencer à réaliser des transactions sécurisées avec le prestataire 33 : pour ce faire, il utilise son dispositif physique 13 pour signer un aléa fourni par le prestataire (on parle alors d'authentification) ou un message (on parle alors de signature) grâce à sa clé secrète S_0, et en y associant le certificat de prestataire correspondant C_i, selon des protocoles standards qui ne font pas l'objet de la présente demande de brevet et ne sont donc pas décrits ici plus en détail.

L'utilisateur 30 peut procéder à un enregistrement 24 auprès de plusieurs prestataires différents, qui délivreront chacun un certificat de prestataire distinct C_i liant la clé publique P_0 du dispositif physique 13 à une identité Id_i de l'utilisateur 30, pertinente pour le prestataire considéré.

REVENDICATIONS

1. Procédé de contrôle de transactions sécurisées mettant en œuvre un dispositif physique (13) détenu par un utilisateur (30) et portant au moins une paire de clés asymétriques, comprenant une clé de dispositif publique (P_0) et une clé de dispositif privée (S_0) correspondante,

caractérisé en ce qu'il comprend les étapes suivantes :

- préalablement à la mise en service dudit dispositif physique, une étape de certification (21) de ladite clé de dispositif publique (P_0) par signature au moyen d'une première clé de certification (S_T) d'une autorité de certification particulière (ACP, 10), délivrant un certificat de dispositif (C_0), après vérification que ladite clé de dispositif privée S_0 est logée dans une zone inviolable dudit dispositif physique (13) ;
- une étape de vérification (22) dudit certificat de dispositif (C_0) au moyen d'une deuxième clé de certification (P_T) correspondant à ladite première clé de certification (S_T) ;
- en cas de vérification positive, une étape d'enregistrement (24) dudit utilisateur (30) auprès d'un prestataire (33) délivrant un certificat de prestataire (C_i) correspondant à la signature par ledit prestataire de ladite clé de dispositif publique (P_0) et d'un identifiant (Id_i) de cet utilisateur (30).

2. Procédé de contrôle selon la revendication 1, caractérisé en ce que ladite autorité de certification particulière (10) est le fabricant dudit dispositif physique (13).

3. Procédé de contrôle selon l'une quelconque des revendications 1 et 2, caractérisé en ce que ledit certificat de dispositif (C_0) est stocké dans une zone (131) de mémoire en lecture libre dudit dispositif physique (13).

4. Procédé de contrôle selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit certificat de dispositif (C_0) signe également au moins une information représentative dudit dispositif physique.

5. Procédé de contrôle selon la revendication 4, caractérisé en ce que ladite information représentative dudit dispositif physique appartient au groupe

comprenant les informations suivantes :

- type de dispositif physique ;
- identification du fabricant dudit dispositif physique ;
- type d'algorithme cryptographique utilisé par ledit dispositif physique ;
- numéro de série dudit dispositif physique.

6. Procédé de contrôle selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ladite étape de vérification (22) est effectuée par ledit prestataire (33).

7. Procédé de contrôle selon l'une quelconque des revendications 1 à 6, caractérisé en ce que ladite première clé de certification (S_T) est une clé privée et ladite deuxième clé de certification (P_T) est une clé publique.

8. Procédé de contrôle selon l'une quelconque des revendications 1 à 6, caractérisé en ce que ladite autorité de certification particulière (10) utilise une clé symétrique (K), de sorte que ladite première clé de certification (S_T) et ladite deuxième clé de certification (P_T) sont identiques.

9. Procédé de contrôle selon la revendication 8, caractérisé en ce que ladite étape de certification est mise en œuvre à partir de ladite clé symétrique par ladite autorité de certification particulière sur requête d'un fabricant dudit dispositif, et en ce que ladite étape de vérification est mise en œuvre par ladite autorité de certification particulière sur requête dudit prestataire.

10. Dispositif physique détenu par un utilisateur et destiné à être utilisé lors de transactions sécurisées, ledit dispositif physique portant au moins une paire de clés asymétriques, comprenant une clé de dispositif publique (P_0) et une clé de dispositif privée (S_0) correspondante,

caractérisé en ce qu'il porte également un certificat de dispositif (C_0), délivré après vérification que ladite clé de dispositif privée S_0 est logée dans une zone inviolable dudit dispositif physique (13), correspondant à la signature de ladite clé de dispositif publique (P_0) par une première clé de certification (S_T) d'une autorité de certification particulière (10),

et en ce que ledit certificat de dispositif (C_0) est stocké dans ledit dispositif

physique préalablement à sa mise en service.

11. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour la mise en œuvre d'au moins une étape du procédé de contrôle de transactions sécurisées selon l'une quelconque des revendications 1 à 9.

12. Système de contrôle de transactions sécurisées sur un réseau de communication (32), mettant en œuvre un dispositif physique (13) détenu par un utilisateur (30) et portant au moins une paire de clés asymétriques, comprenant une clé de dispositif publique (P_0) et une clé de dispositif privée (S_0) correspondante,

caractérisé en ce qu'il comprend au moins :

- un serveur de certification particulière (35) relié audit réseau, délivrant audit dispositif physique, après vérification que ladite clé de dispositif privée S_0 est logée dans une zone inviolable dudit dispositif physique (13) et préalablement à sa mise en service, un certificat de dispositif (C_0) correspondant à la signature de ladite clé de dispositif publique (P_0) par une première clé de certification (S_T) dudit serveur de certification particulière (35) ;
- un serveur de vérification (34) dudit certificat de dispositif (C_0) au moyen d'une deuxième clé de certification (P_T) correspondant à ladite première clé de certification (S_T), ledit serveur de vérification étant relié audit réseau ;
- un serveur d'enregistrement (33) dudit utilisateur (30) auprès d'un prestataire, délivrant audit utilisateur (30), en cas de vérification positive par ledit serveur de vérification, un certificat de prestataire (C_i) correspondant à la signature par ledit prestataire de ladite clé de dispositif publique (P_0) et d'un identifiant (Id_i) dudit utilisateur, ledit serveur d'enregistrement étant relié audit réseau.

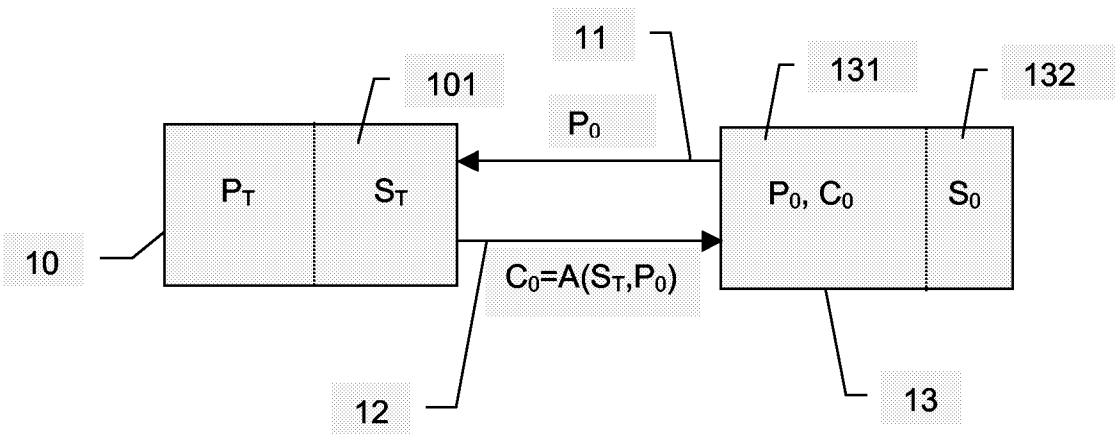


FIGURE 1

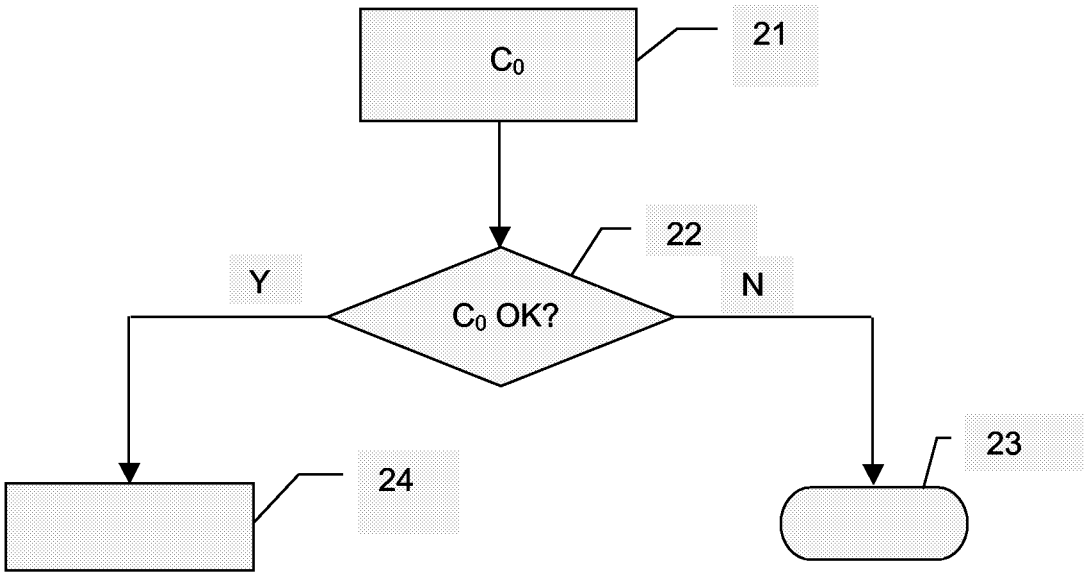


FIGURE 2

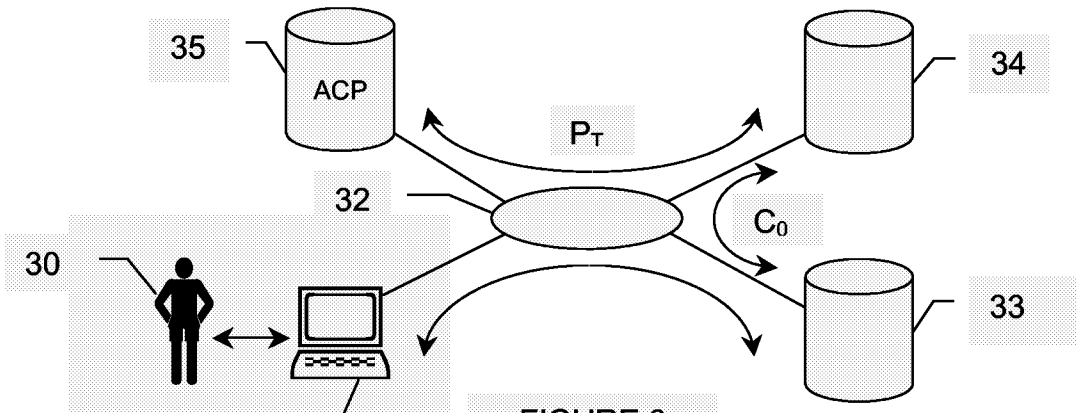


FIGURE 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/064383

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC , XP002376605 page 491 page 547 - page 549 page 559 - page 560 page 572 - page 576	1-12
X	US 2003/097592 A1 (ADUSUMILLI KOTESHWERRAO) 22 May 2003 (2003-05-22) abstract paragraph [0035] - paragraph [0036]	1-12
A	US 5 903 721 A (SIXTUS ET AL) 11 May 1999 (1999-05-11) abstract figures 1,2 column 3, line 26 - column 5, line 31	1-12

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 September 2006	19/09/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	SAN MILLAN MAESO, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/064383

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01/16900 A (AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY,) 8 March 2001 (2001-03-08) abstract -----	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/064383

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003097592 A1	22-05-2003	CN 1575579 A	02-02-2005
		DE 10297362 T5	09-09-2004
		GB 2395877 A	02-06-2004
		HK 1062752 A1	07-10-2005
		US 2003081783 A1	01-05-2003
		WO 03036913 A2	01-05-2003
US 5903721 A	11-05-1999	AU 6549498 A	29-09-1998
		BR 9809045 A	22-01-2002
		CA 2283933 A1	17-09-1998
		DE 1008022 T1	25-01-2001
		EA 1825 B1	27-08-2001
		EP 1008022 A2	14-06-2000
		ES 2150892 T1	16-12-2000
		JP 2001518212 T	09-10-2001
		NO 994428 A	09-11-1999
		WO 9840809 A2	17-09-1998
WO 0116900 A	08-03-2001	AT 258328 T	15-02-2004
		AU 775976 B2	19-08-2004
		AU 7090700 A	26-03-2001
		AU 2004231226 A1	23-12-2004
		BR 0013822 A	23-07-2002
		CA 2382922 A1	08-03-2001
		CN 1376292 A	23-10-2002
		CZ 20020744 A3	18-02-2004
		DE 60007883 D1	26-02-2004
		DE 60007883 T2	14-10-2004
		DK 1212732 T3	07-06-2004
		EP 1212732 A2	12-06-2002
		ES 2215064 T3	01-10-2004
		HK 1048550 A1	21-10-2004
		HR 20020180 A2	30-06-2004
		HU 0202471 A2	28-11-2002
		JP 2003508838 T	04-03-2003
		MA 27459 A1	01-08-2005
		MX PA02002081 A	30-07-2004
		NO 20020996 A	24-04-2002
		NZ 517840 A	24-03-2005
		PL 353773 A1	01-12-2003
		PT 1212732 T	30-06-2004
		TR 200201280 T2	21-08-2002
		TR 200202436 T2	21-01-2003
		TW 548564 B	21-08-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2006/064383

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC , XP002376605 page 491 page 547 - page 549 page 559 - page 560 page 572 - page 576	1-12
X	US 2003/097592 A1 (ADUSUMILLI KOTESHWERRAO) 22 mai 2003 (2003-05-22) abrégé alinéa [0035] - alinéa [0036]	1-12
A	US 5 903 721 A (SIXTUS ET AL) 11 mai 1999 (1999-05-11) abrégé figures 1,2 colonne 3, ligne 26 - colonne 5, ligne 31	1-12

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
12 septembre 2006	19/09/2006

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	SAN MILLAN MAESO, J

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2006/064383

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 01/16900 A (AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY,) 8 mars 2001 (2001-03-08) abrégé -----	1-12

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2006/064383

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2003097592 A1	22-05-2003	CN 1575579 A	02-02-2005
		DE 10297362 T5	09-09-2004
		GB 2395877 A	02-06-2004
		HK 1062752 A1	07-10-2005
		US 2003081783 A1	01-05-2003
		WO 03036913 A2	01-05-2003
US 5903721 A	11-05-1999	AU 6549498 A	29-09-1998
		BR 9809045 A	22-01-2002
		CA 2283933 A1	17-09-1998
		DE 1008022 T1	25-01-2001
		EA 1825 B1	27-08-2001
		EP 1008022 A2	14-06-2000
		ES 2150892 T1	16-12-2000
		JP 2001518212 T	09-10-2001
		NO 994428 A	09-11-1999
		WO 9840809 A2	17-09-1998
WO 0116900 A	08-03-2001	AT 258328 T	15-02-2004
		AU 775976 B2	19-08-2004
		AU 7090700 A	26-03-2001
		AU 2004231226 A1	23-12-2004
		BR 0013822 A	23-07-2002
		CA 2382922 A1	08-03-2001
		CN 1376292 A	23-10-2002
		CZ 20020744 A3	18-02-2004
		DE 60007883 D1	26-02-2004
		DE 60007883 T2	14-10-2004
		DK 1212732 T3	07-06-2004
		EP 1212732 A2	12-06-2002
		ES 2215064 T3	01-10-2004
		HK 1048550 A1	21-10-2004
		HR 20020180 A2	30-06-2004
		HU 0202471 A2	28-11-2002
		JP 2003508838 T	04-03-2003
		MA 27459 A1	01-08-2005
		MX PA02002081 A	30-07-2004
		NO 20020996 A	24-04-2002
		NZ 517840 A	24-03-2005
		PL 353773 A1	01-12-2003
		PT 1212732 T	30-06-2004
		TR 200201280 T2	21-08-2002
		TR 200202436 T2	21-01-2003
		TW 548564 B	21-08-2003